др Маринка Цетинић
доцент Правног факултета Универзитета у Београду

РЕШЕЊЕ КОМПЈУТЕРСКИХ КРИВИЧНИХ ДЕЛА У НОВОМ КРИВИЧНОМ ЗАКОНИКУ РУСКЕ ФЕДЕРАЦИЈЕ

I

1. Сагледавању правних аспеката употребе компјутера приступило се од момента примене компјутерске технике и технологије 70 и 80-тих година овога века. Наравно, као недовољно истражена и нова област науке, и у најразвијенијим земљама света, правно проучавање компјутерског и технолошког аспекта није одмах добило своје потребно место. Чак и технолошки најразвијеније земље, у којима је компјутерска делатност нашла широку примену, питању правне заштите, а поготову, питању спречавања компјутерског криминалитета, нису приступиле одмах. Било је потребно извесно време да би се схватила неопходност правног регулисања употребе компјутера, а затим, кривичноправна заштита злоупотребе технике и технологије. Наиме, тек временом се показало да велику опасност представља несанкционисан приступ информацијама, уношење и уништавање информација, уношење вируса у компјутер, модификација компјутерских материјала. Ипак, већ 1973. године у Шведској је донет пропис који познаје кривичноправну заштиту од компјутерског криминалитета, (Sweidich Data Act, допуњен 1982. године), у којем је у чл. 21. предвиђено дело „неовлашћени програмски приступ" као кривично дело недопуштеног, противзаконитог приступа подацима (1). У Аустралији, у држави Викторија, донет је 1988. године компјутерски закон у коме је било предвиђено кривично дело „компјутерског неовлашћеног упада" (чл. 9.), као недозвољено прибављање приступа или улаза у компјутерски систем или део компјутерског система без законског овлашћења (2). Године 1986. Конгрес САД донео је „Закон о преварама и злоупотребама које се остварују помоћу компјутера". (3)

---

(1) др З. Мршевић, *Компјутерски криминалитет и потреба конципирања кривичног дела компјутерске злоупотребе*, ЈРКК 1/1991, стр. 70.

(2) *Ibidem.*

(3) *Новое уголовное право Росии*, Особенная част, Москва, 1996, стр. 273.

Најзад, у Великој Британији је 1990. године ступио на снагу „Закон о злоупотреби компјутера" са предвиђеним кривичним делима: компјутерске злоупотребе или недозвољени приступ програму или подацима садржаним у компјутеру (4).

2. Нема велике потребе за навођење чињенице да је опасност од компјутерских кривичних дела изузетно велика. По неким проценама стручњака губици проузроковани овим кривичним делима у свету достижу 5 милијарди долара годишње. Тако је, на пример, у САД извесни A. Kebs, уз учешће помагача, извршио велику пљачку банке у Даласу, тако што је ушао у компјутерски електронски систем банкарских операција и, затим, пренео више од 70 милиона долара у две банке у држави Лихтенштајн (5). Група хакера је открила приступ у више од 50 аутоматизованих банака података (Лос-Аламоској нуклеарној лабораторији, великом еколошком центру и другим објектима САД). Најзад, као пример може се навести и дело R. Moriss-a који је заразио вирусом више од 6 хиљада компјутера и 70 компјутерских центара, међу којима су били компјутерски систем NASE, Ливерморска лабораторија за нуклеарна истраживања, као и највиши универзитетски центри САД (6).

Све ово говори у прилог става да је потребно у свим земљама, како технолошки најразвијенијим тако и оним које тај назив не могу да понесу, али, које су ипак почеле са увођењем технологија и компјутеризацијом, успоставити једну свеобухватну заштиту ове области и предвидети законске прописе у којима ће јасно бити издиференцирани различити облици компјутерских кривичних дела. Нема сумње да је појава електронске рачунске технике већ четврте и пете генерације, као и примена ових система у свим областима унутар једног друштва (управа, привреда, наука, банкарство итд.) у тој мери повећала значај информација да се кривичноправна заштита од злоупотреба разних врста наметнула.

II

3. Руско друштво, по много чему је било слично нашем. Карактерисала га је дугогодишња изолованост у области привреде и другим областима, да би тек након друштвених промена које су извршене крајем 80-тих година, дошло и до промена у привреди,

(4) др З. Мршевић, *Нове законске одредбе о злоупотреби компјутера у Великој Британији*, Страни правни живот, 2–3/1990, стр. 43.

(5) Новое уголовное право Росии, *op. cit.* стр. 273.

(6) Новое уголовное право Росии, *op. cit.* стр. 272.

преласка на тржишну економију и широке примене нових технологија. Међутим, са осавремењавањем пословања и увођењем компјутерске технологије није дошло до одговарајуће регулативе, било у области грађанског, било управног права, а поготово не у области кривичног права. Постепено, након доношења прописа из других грана права, којима се регулише ова материја, настали су и услови за доношење одговарајућих прописа из области кривичног права, односно, утврђивање кривичноправне заштите. Први закон којим је пружена заштита компјутерској технологији, донет је 23. новембра 1992. године: „О правној заштити програма за електро-рачунске машине и базе података" (7). Други, важан пропис донет је 20. фебруара 1995. године — „Федерални закон о информацији, информисању и заштити информације" (8). На крају, ступањем на снагу Кривичног Законика Руске Федерације 24. новембра 1995. године уведена је посебна, нова глава Законика — „Кривична дела у сфери компјутерске информације". (9) У Законику су инкриминисана три кривична дела: 1.) противправни приступ компјутерској информацији (чл. 258.); 2.) прављење, коришћење и пласман вирусних програма (чл. 269) и 3.) коришћење правила експлоатације компјутерског система или мреже (чл. 270.). Тиме је, коначно, завршен пут ка увођењу кривичноправне заштите од компјутерског криминалитета.

4. Посебни део новог Законика Руске Федерације подељен је на дванаест делова, од којих девети део, који обухвата кривична дела компјутерске злоупотребе, носи наслов „Кривична дела против друштвене безбедности и друштвеног поретка."

Део Законика којим су инкриминисана кривична дела компјутерског криминалитета смештен је у главу двадесет осам, одељак девет, чиме је законодавац одредио шири заштитни објекат кривичних дела у сфери компјутерске информације. Дакле, друштвена безбедност у целини и друштвени поредак, по систематизацији Законика, представља заштитни објекат компјутерских кривичних дела. Међутим, по много чему би требало да ова кривична дела имају један ужи заштитни објекат као скуп друштвених вредности и односа везаних за производњу, коришћење, пласман и заштиту информације и информационих система. Да је то уочио и руски законодавац показује назив главе двадесет осам — кривична дела у сфери информације. Нападом на ове објекте заштите у крајњем се напада на друштвену безбедност и друштвени поредак. Међутим, и свим другим кривичним делима из посебног дела Кривичног

(7) Новое уголовное право Росии, *op. cit.* стр. 273.

(8) *Ibidem.*

(9) *Ibidem.*

Законика Руске Федерације, као и овим, у крајњем се напада на широко одређене друштвене вредности. Толико широко одређен заштитни објекат може се, можда, објаснити тиме да нарушавање рада програма аутоматизованог система управљања виталних објеката привреде, саобраћаја, војног потенцијала и тако даље, може довести до угрожавања (да ли баш?) друштвене безбедности и друштвеног поретка земље. Можда је то последица чињенице скорог инкриминисања ових дела и њиховог недовољно издиференцираног ширег објекта заштите. С друге стране, можда је то последица и чињенице да су се у том, као најопштијем одељку, нашле све групе кривичних дела за које није било места у неким другим одељцима Законика. Требало би, изгледа, да овај шири заштитни објекат буде уже одређен, јер би у складу са таквом систематизацијом, и многа друга кривична дела требало да нађу место у овом одељку Кривичног Законика.

5. Нападни објекат ове групе кривичних дела представља укупност информационих и апаратских структура. Компјутери као информациона структура, носиоци информација, представљају објекте којима се чини штета од противправног приступа информацији, уништења и пласмана вирусног програма и најзад, кршења правила експлоатације компјутерског система или мреже. Треба нагласити да компјутер може бити нападни или граматички објекат кривичних дела против имовине (крађа компјутера, уништење или оштећење), када се квалификација дела врши по одредбама чланова из групе кривичних дела против имовине (чл. 158–168. КЗ Руске Федерације). Међутим, руски законодавац је јасно уочио да програм не може бити нападни објекат групе кривичних дела против имовине јер не располаже физичким карактеристикама — да је покретна ствар која би се могла одузети, присвојити или уништити (крађа, утаја или оштећење ствари). У групи кривичних дела у сфери компјутерске информације нападни објекат је компјутер као информациона структура, носилац информације, док сам компјутер представља средство за вршење свих кривичних дела у рукама учиниоца.

III

6. У оквиру главе „Кривична дела у сфери компјутерске информације" руски законодавац је предвидео три нова кривична дела.

7. Прво дело „Противправни приступ компјутерској информацији", предвиђен у чл. 268. КЗ Руске Федерације у основном

облику гласи: „Противправни приступ информацији у компјутерски систем или мрежу, и такође, намерни унос у компјутерски систем или мрежу лажне информације, кажњава се новчаном казном у распону од две до пет стотина минималне цене рада, или у нивоу личног дохотка, или другог прихода осуђеног у трајању од два до пет месеци, или поправним радом у трајању од шест месеци до једне године, или затвором у трајању од два до четири месеца."

Основни облик кривичног дела предвиђен је у две алтернативне одређене радње извршења: 1) противправни приступ информацији у компјутерском систему или мрежи и 2) намерно увођење у компјутерски систем или мрежу лажне информације.

Први облик радње представља могућност располагања информацијом, односно приступ било ком програму или подацима садржаним у компјутеру од стране лица које за то није овлашћено. Начини приступа су многобројни и само примера ради могу се навести коришћење туђег имена, промена физичких односа техничких инсталација, модификација програмског и информационог обезбеђења, „пробијање" заштите система и тако даље. Приступ мора бити противправан, што значи да учинилац није овлашћен на било који начин приступу програмима или информацијама. Такође, учинилац ће бити одговоран за приступ информацији у компјутерском систему или мрежи и када не поседује пристанак или дозволу лица које је овлашћено да даје дозволе. Док се недостатак овлашћења лако утврђује када су у питању лица са стране, тј. када је у питању приступ са дистанце, када је у питању лице изнутра, постаје дискутабилно да ли је његов приступ био овлашћен и ко треба да му да овлашћење за њега (10). Противправан приступ компјутерској информацији сматра се довршеним делом моментом добијања могућности коришћења информације (11). Супротно тумачењу кривичног дела недозвољеног приступа програму или подацима садржаним у компјутеру, из Закона о злоупотреби компјутера из 1990. године Велике Британије, заступају Wasil и др. З. Мршевић (12). Чини се да је исправнији став да је ово врло широко конципирано кривично дело те се за њега не захтева да је довршена предузета радња и да је наступила последица. Већ и сам покушај, тј. свако активирање компјутера, па чак само активирање сигурносног система компјутера, представљало би радњу овог кривичног

(10) Др З. Мршевић: *Заштита приватности од злоупотребе компјутера — потреба кривичноправне регулативе*, ЈРКК, 4/1991.

(11) Новое уголовное право Росии, *op. cit.*, стр. 276.

(12) Суштина овог кривичног дела је тако конципирана да представља кажњив покушај јер се практично ради о „куцању на врата циљног компјутера"; др З. Мршевић, *Заштита приватности од злоупотребе компјутера — потреба кривичноправне регулативе*, *op. cit.*, стр. 142.

дела. Група аутора, приликом тумачења одредбе чл. 268. КЗ Руске Федерације, и сама уочава да је „конструкција бића кривичног дела по принципу „формалног кривичног дела" доста спорна, јер се неосновано безгранично проширује сфера употребе чл. 268., у том смислу и на случајеве потпуног одсуства неких друштвено опасних последица". (13)

Ово кривично дело може се учинити само умишљајем.

Други облик радње овог кривичног дела представља намерно уношење у компјутерски систем или мрежу лажне информације. Делатности којима се може остварити овај облик радње кривичног дела из чл. 268. могу бити на пример измена информације о нечему, уношење измена у програм система које могу представљати допунске команде које ће функционисати само у одређеним условима или које у потпуности или делимично избацују из система компјутерски систем.

Овај облик кривичног дела може се учинити само са умишљајем, с тим што је код учиниоца потребна и намера уношења лажне информације.

Учинилац овог кривичног дела може бити свако лице.

Кривично дело може бити учињено само са умишљајем.

8. Друго кривично дело „Прављење, коришћење и пласман вирусних програма", предвиђено чл. 269. Кривичног Закона Руске Федерације, у основном облику гласи: „Прављење компјутерских програма или уношење измена у постојећим компјутерским програмима које доводи до несанкционисаног уништења, блокирања, модификације, копирања информација или ометање рада компјутерске опреме, такође коришћење или пласирање носача са таквим програмима казниће се лишењем слободе у трајању од четири године и новчаном казном од две до пет стотина минималне цене рада, или у обиму личног дохотка, или другог дохотка осуђеног у трајању од два до пет месеци."

Ово кривично дело предвиђено је у неколико алтернативно одређених облика радње којима се од вируса штите информације, информациони систем и информациона мрежа. Наиме, ове вредности се штите од радњи којима се проузрокује уништење, блокирање, модификација компјутерске информације или ометање рада компјутерске мреже или коришћење или пласирање носача са вирусним програмима. Вируси, као и вирусни програми, који за разлику од вируса, не оштећују нити уништавају постојеће програме, али заузимају комплетно компјутерску меморију чиме га оне-

(13) ' Новое уголовное право Росии, *op. cit.*, стр. 276.

могућавају да функционише, располажу способношћу да прелазе кроз комуникационе мреже из једног система у други. Вируси и вирусни програми шире се као вируси који се током одређеног времена не примећују да би, након оболевања компјутера, компјутер испао из система рада. Последица уношења вирусног програма у компјутер може бити потпуно уништење информација.

Први облик радње представља у потпуности прављење вирусног програма.

Други, алтернативно одређени, облик радње овог кривичног дела је уношење измена у већ постојеће програме (уношење вируса).

Трећи, алтернативно одређени, облик је коришћење вирусних програма који може учинити како сам аутор, тако и други корисници за нпр. заштиту своје програмске конфигурације и информације од крађе, или за заражење других компјутера.

Најзад, последњи алтернативно одређени, облик радње овог кривичног дела је планирање вирусног носача програма, што значи њихово давање другим корисницима компјутерског система или мреже.

Последице овог кривичног дела су јасно одређене као: уништење, блокирање, модификација, копирање информација или ометање рада компјутерске опреме. Отуда следи да се кривично дело довршава моментом наступања наведених последица.

Сви наведени облици радње овог кривичног дела подразумевају да је очувана физичка целовитост компјутерског система.

Учинилац кривичног дела може бити свако лица, а кривично дело се може учинити само са умишљајем.

9. Најзад, последње предвиђено кривично дело, из чл. 270. Кривичног Законика Руске Федерације, носи наслов „Кршење правила експлоатације компјутерског система или мреже". Предвиђено је у основном облику као „Кршење правила експлоатације компјутерског система или мреже од стране лица које има приступ том систему или мрежи, ако је то проузроковало уништење, блокаду, модификацију компјутерске информације или ометање рада компјутерске опреме, казниће се лишењем права бављења одређеним дужностима или бављењем одређеном делатношћу у трајању од пет година."

Основни облик овог кривичног дела може бити учињен, као и свако кршење правила, било чињењем било нечињењем (кршење правила експлоатације компјутерског система или мреже). Делатности, било као чињење било као нечињење, изражавају се у облику непоштовања, неадекватног поступања или директног кр-

шења одређених правила који се тичу безбедности рада компјутерског система или мреже.

Последица овог кривичног дела је уништење, блокада, модификација компјутерске информације или ометање рада компјутерске опреме. Према томе, кривично дело се сматра довршеним моментом наступања наведених последица.

Кривично дело може бити учињено само са умишљајем, при чему мотиви учиниоца могу бити различити, као нпр. „спортски" интерес, освета, користољубље итд. који се узимају у обзир приликом одмеравања казне.

Активни субјекат овог кривичног дела, за разлику од претходна два, је специфичан: лице које има приступ компјутерском систему или мрежи. То могу бити нпр. програмери, оператери на рачунарима, мајстори опреме, нека посебна службена лица.

10. За сва три облика кривичних дела руски законодавац је предвидео и теже облике.

Чл. 268. у ст. 2. садржи три квалификована облика уколико основни облик кривичног дела има за последицу: а) модификацију, уништење, блокирање или копирање информације или избацивање из система компјутерске опреме; б) ако су извршени од стране групе лица уз претходни договор или ако су извршени од стране организоване групе и в) ако су извршени од стане лица које има приступ компјутерском систему или мрежи, кажњавају се новчаном казном у износу од пет стотина до осам стотина минималних личних доходака, или у нивоу личног дохотка, или другог дохотка осуђеног у року од пет до осам месеци, или се кажњавају поправним радом у трајању од једне године до две године, или казном затвора у трајању од три до шест месеци, или лишењем слободе у периоду до две године. У ст. 3. чл. 268. предвиђен је најтежи облик као: „Радње предвиђене у ставовима 1. и 2. овог члана које су учињене у погледу информације ограниченог приступа, које се налази у машинском носачу, у компјутеру, компјутерском систему или мрежи, које су подједнако повукле тешке последице, казниће се лишењем слободе у трајању до пет година."

Чл. 269. у ст. 2. предвиђа само један квалификовани облик и то: „Исте радње које су проузроковале теже последице, казниће се лишењем слободе од три до седам година."

Најзад, у чл. 270. предвиђена су у ст. 2. три тежа облика овог кривичног дела и то: а) ако су радње учињене у погледу компјутерског система или мреже које садрже информацију ограниченог приступа, б) ако су учињене од стране групе лица уз претходни договор или уколико је учињена радња од стране организоване

групе и в) уколико је радња проузроковала тешке последице, казниће се лишењем слободе у трајању до четири године.

Међу квалификованим околностима издваја се вршење основних дела од стране групе уз претходни договор или од стране организоване групе. Под информацијом ограниченог приступа подразумева се информација којом има право располагања само њен власник, чије објављивање, уништење или блокирање може да нанесе озбиљне губитке интересима целог друштва (нпр. подаци који чине државну тајну), било уставним правима грађана на чување личне тајне и права на тајност личних података (нпр. подаци о оболелима од HIV вируса). Најзад, у тешке последице се, према мишљењу групе аутора, убрајају чињење велике штете, озбиљно нарушавање делатности предузећа, организација и установа, проузроковање хаварија, катастрофа, проузроковање штетности по здравље људи (14).

IV

11. Нови Кривични Законик Руске Федерације по много чему, када је у питању компјутерски криминалитет, узима у обзир савремене трендове у овој области. Наравно, иако се примећује недовољна прецизност, гломазност појединих бића кривичних дела, ипак је за сваку похвалу чињеница да руски законодавац није остао нем пред развитком нове компјутерске технологије. Одговарајућа законска регулатива је донета након уочавања облика и типова злоупотребе компјутерских система и мрежа уз коришћење искустава у технолошки развијенијим системима.

Чињеница је, међутим, да примена компјутера код нас није ишла паралелно са његовим технолошким развитком, да би тако постепено и законодавство сазревало пратећи појаву потребе регулисања појединих аспеката његове примене (15). Иако је компјутер тек задњих година ушао у масовну употребу, то није довољно оправдање за нашег законодавца да не приступи правном регулисању употребе компјутерске технологије. Навођење упоредноправних примера има за циљ апел да се код нас не чека десет или двадесет година, већ да се већ искристалисане дефиниције и појмови усвоје у некој прихватљивој форми (16). Стога је и овај приказ и анализа компјутерских кривичних дела у Кривичном Законику Руске Федерације имала за циљ указивање на могуће облике

(14) Новое уголовное право Росии, *op. cit.*, стр. 277.

(15) Др З. Мршевић, *Заштита приватности од злоупотреба компјутера — потреба кривичноправне регулативе*, *op. cit.*, стр. 145.

(16) *Ibidem.*

кривичноправне заштите од компјутерског криминалитета. За надати се да ће законодавна комисија која припрема нацрт новог кривичног законика СР Југославије узети у обзир многобројне радове наших научника, који сви имају за задатак помоћ законодавцу у регулисању ове области. Наш законодавац би тако, могао узети у обзир и ово ново (савремено) решење, иако је јасно да ће његова оцена бити комплетнија тек провером учињеном од стране праксе, за шта је потребно једно дуже време од веома кратког времена које је протекло од ступања на снагу Кривичног Законика Руске Федерације до писања овог текста. У сваком случају, овај рад је покушај да се предложи једно ново решење заштите од компјутерског криминалитета у моменту очекивања реформе нашег кривичног законодавства.